SPACE CYBERSECURITY WEEKLY WATCH

W37

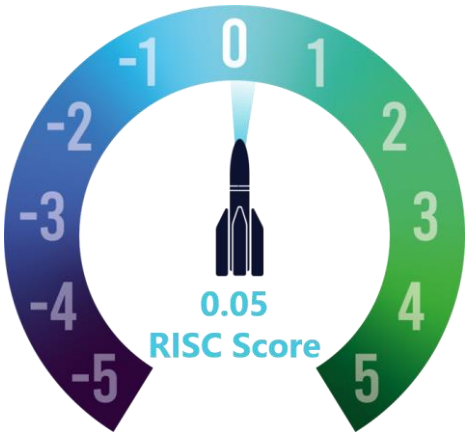
September 8 – September 14, 2026

Timeframe: Weekly
# of news identified: 25
Est. time to read: 40 minutes

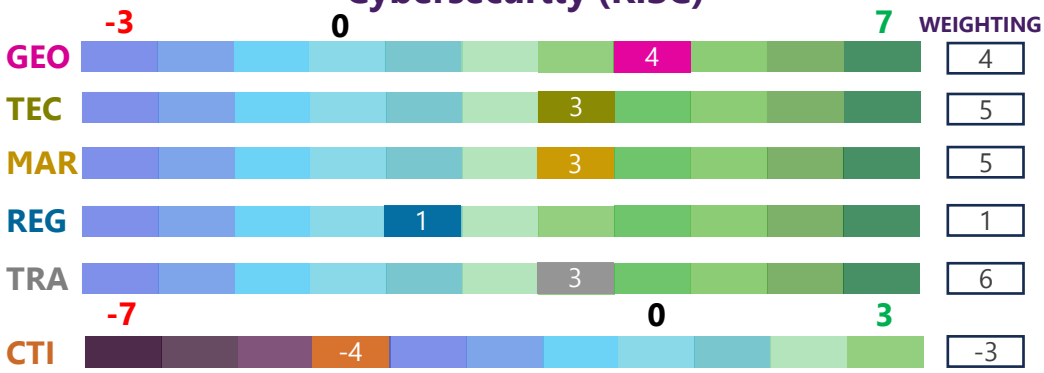
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

- GEOPOLITICS
- TECHNOLOGY
- MARKET & COMPETITION
- REGULATION
- TRAINING & EDUCATION
- THREAT INTELLIGENCE
- IMPORTANT NEWS

RISC Score Assessment

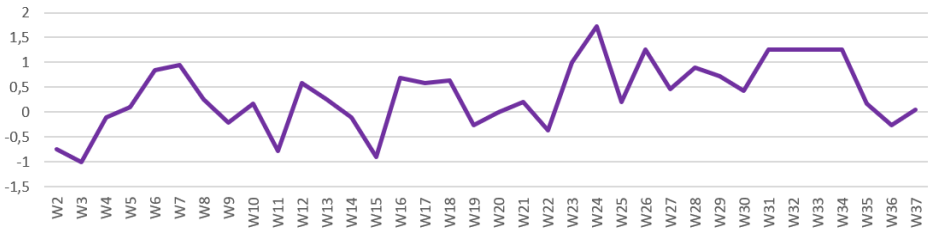


Overview & Resilience Index for Space Cybersecurity (RISC)



The RISC score for this watch is 0.05, a 0.32 increase from last week. This is primarily due to several major strategic initiatives that are setting the stage for a trend toward strengthening cybersecurity measures in the space sector.

RISC Score evolution in 2026



This week's developments highlight the accelerating militarization and securitization of space, with Europe and the UK taking bold steps to expand their space defense capabilities. **Paris hosted the first European Space Defense Forum**, bringing together defense officials from 30 countries to transition from cooperation to the development of military capabilities in space, signaling a shift toward collective defense in orbit. The **UK's £7.8 billion space strategy** aims to protect critical infrastructure, with a significant portion allocated to boosting space intelligence, surveillance, and reconnaissance to counter enemy activity and safeguard satellites. Meanwhile, **Germany is assessing ground-based electronic warfare systems** to disrupt Russia's Rassvet satellite network, reflecting growing concerns over adversarial space capabilities. On the technological front, **SpiderOak's OrbitSecure** introduces a zero-trust cybersecurity solution to protect space-based communications and address vulnerabilities in distributed satellite architectures. In the U.S., the **White House and Space Force's priorities emphasize the need for resilient infrastructure** in a contested domain, as space becomes increasingly vital for communications, navigation, and national security. Lastly, **expert discussions on managing critical ground infrastructure** underscore the importance of securing terrestrial systems that support orbital operations to ensure resilience in contested environments.

GEOPOLITICS

European Space Defense: Paris wants to move from cooperation to military capability

Europe is beginning to organize its space defense in the same way it already organizes its air and cyber defense. Gathering in Paris on the sidelines of the International Space Summit, defense officials from some 30 countries participated in the first edition of the European Space Defense Forum. Seated around the table were the member states of the European Union, as well as Ukraine, the United Kingdom, Norway, and Switzerland. **#EuropeanSpaceDefense #MilitaryCapabilities**

Source: BusinessTimes

MARKET & COMPETITION

UK moves to expand military space capabilities with £7.8bn strategy

The Defense Secretary launched a new space strategy to protect critical space infrastructure, which, if disabled, could cripple the UK economy. The Government pledged £7.8bn for space, including an £880m pot to boost UK space intelligence, surveillance, and reconnaissance capabilities to track enemy activity and stop attacks on satellites.

#Strategy #CyberspaceWarfare

Sources: AOL, The Defense Watch, RNTFND

[redacted]

REGULATION

[redacted]

Securing the high frontier: the White House & the Space Force's priorities for exploration & defense in a contested domain

Space has entered a new era. What was once primarily a sphere of scientific inquiry and exploration evolved into an economic engine, essential infrastructure layer, and disputed national security environment. Communications, navigation, weather forecasting, intelligence, financial transactions, precision agriculture, disaster response, and military activities are increasingly reliant on space systems and the terrestrial networks that connect them. **#WhiteHouse #ContestedDomain**

Source: GOVCONWire

[redacted]

THREAT INTELLIGENCE

Germany seeks counter-space systems to neutralize Russia's Rassvet network

Germany's armed forces are assessing ground-based electronic warfare systems capable of disrupting satellite navigation and communications, as Russia develops its Rassvet satellite network. **#Germany #RassvetNetwork**

Sources: United24media, hartpunkt, Defence Express

[redacted]

[redacted]

Source: [redacted]

[redacted]

[redacted]

Source: [redacted]

[redacted]

[redacted]

Source: [redacted]

[redacted]

[redacted]

Source: [redacted]

[redacted]

[redacted]

Source: [redacted]

TECHNOLOGY

SpiderOak Orbitsecure brings zero-trust cybersecurity to space-based communications

SpiderOak's OrbitSecure is a zero-trust cybersecurity solution designed to protect commands and data across space-based communications and distributed satellite architectures. Rather than relying on trusted networks or third-party infrastructure, OrbitSecure applies access controls directly to data using Secure Data Compartments (SDCs). **#SpiderOak #OrbitSecure**

Source: SATNow

[redacted]

[redacted]

Source: [redacted]

[redacted]

[redacted]

Source: [redacted]

TRAINING & EDUCATION

GNSS spoofing and jamming detection and mitigation in smart city architecture

This paper examines the role of GNSS in smart city architecture, surveys the jamming and spoofing threat landscape, and reviews current detection techniques spanning signal-level monitoring, cryptographic authentication, spatial antenna array processing, and data-driven machine learning approaches. #GNSS #Detection

Source: IRJmanuals



Cybersecurity risks in satellite ground segment infrastructure: threat profiling and analysis

This paper examines cybersecurity risks within satellite ground segment infrastructure through structured threat profiling and risk analysis. #AmosAdeiza #ThreatProfiling

Source: IRJmanuals



Ransomware resilience and the space industry – Cyber Revolution Summit Thailand 2026

A satellite mission is not only about spacecraft - it depends on ground stations, mission control, cloud platforms, servers, partners, and user terminals. One compromised trusted connection can threaten data integrity, mission continuity, and downstream services. #Summit #RansomwareResilience

Source: LinkedIn



Space cyber defense – know your systems, know your adversary: threat intelligence meets cyber risk exposure management.

Marco Schmidt from Trend AI presents vulnerabilities and methods used by attackers to target satellites and mobile ground stations. #SpaceCyberDefence #TrendAI

Source: LinkedIn

Defending the orbital infrastructure: Cyber resilience in the Euro-Atlantic space industry

Luciano Maggiò Sordello expands on its article Attacchi Cyber all'Industria Spaziale. Difendiamoci Prima del Disastro, published in Agenda Digitale, and reframes the argument within peer-reviewed research on space systems security, critical infrastructure protection and resilience governance. #SpaceDefence #ResearchArticle

Source: European Open University



A framework for secure, low-latency communication in mobile Nigerian military operations

This study proposes a framework for secure, low-latency communication in mobile Nigerian military operations. The framework integrates adaptive routing mechanisms, optimized encryption techniques, and resilient network architecture to balance security requirements with communication efficiency. #ResearchPaper #Nigeria

Source: InternationalJournalofScientificResearchandManagement



Working session on cyber architecture development in the Defense Security Cooperation University (DSCU) Cyber Team

A researcher, Adnom Nugaid, had the opportunity to join the Defense Security Cooperation University (DSCU) to deliver a talk on satellite cybersecurity. #DSCU #Malaysia

Source: LinkedIn



Network-centric territoriality in low earth orbit: pre-gray zone operations and the infrastructure of orbital sovereignty

In an era of expanding satellite constellations and increasing strategic competition in the space domain, could the most consequential contests in Low Earth Orbit be fought over access and connectivity rather than territory itself? #NetworkCentricTerritoriality #PreGrayZoneOperations

Source: LinkedIn

TRAINING & EDUCATION

Managing critical ground infrastructure in contested environments

Ben Pigsley, President & CEO at US Electrodynamics Inc. (USEI), will share insights on one of the industry's most important topics at USEI about managing critical ground infrastructure in contested environments. **#USEI #WorldSPaceBusinessWeek**

Source: Linkedin

[redacted]

CyberInflight is a Market Intelligence company dedicated to the topic of Space Cybersecurity. The company provides strategic market and research reports, bespoke consulting, market watch & OSINT research, and cybersecurity awareness training.
Contact us at: research@cyberinflight.com